LA CIBERGUERRA. GÉNESIS Y EVOLUCIÓN

Julio ALBERT FERRERO

(2.ª RR)

Introducción

ESTE artículo trata de la evolución de los ataques que constantemente se generan en el ciberespacio, cuyo nivel más alto sería la ciberguerra, dotada de una gran sofisticación, consecuencia del rápido incremento tecnológico en este ámbito. Para ello haré un recorrido que comenzará por la definición de los conceptos fundamentales, pasaré por la situación actual en el ciberespacio en el ámbito militar, internacional y de la OTAN, y finalizaré con los ciberataques más importantes de los últimos tiempos.

Las nuevas tecnologías han venido a complicar la seguridad de las naciones y de sus infraestructuras a través del ámbito cibernético, o sea en el ciberespacio. Este es un territorio factible de ser dominado, al igual que la tierra, el mar, el aire y la alta atmósfera (conocidos como los *Globals Commons*), en lo relativo a la guerra. El ciberespacio estará presente en cualquier guerra que se produzca en el futuro; se puede utilizar como arma militar, aunque normalmente limitado en el tiempo, pero también se puede emplear para el espionaje, en cuyo caso el tiempo pierde importancia. Al igual que la mar no puede dominarse sino de una manera relativa, conceptualmente el *Dominio Relativo del Mar* ha venido a sustituir al *Dominio del Mar*. Así, en caso de conflicto armado la situación normal será la de dominio compartido. Es el arma del débil por antonomasia, como la mina, y aunque no tiene identidad física su influencia es cada vez más importante. Es una realidad virtual de la que forman parte los ordenadores, servidores y redes del mundo, no es un espacio físico sino conceptual, por donde circulan datos, y donde se producen los ataques, conocidos como ciberataques, que son las acciones de la ciberguerra, ante los que es preciso reaccionar mediante acciones de defensa cibernética, objeto de la Estrategia de Ciberdefensa.

Este espacio virtual, que incluye a Internet y las redes militares y comerciales, es por lo tanto un campo de batalla de enormes dimensiones, que asegura el anonimato y sobre el que se puede operar desde cualquier parte del mundo. La posibilidad de conexión con cualquier sistema lo convierte en un objetivo susceptible de ser atacado. La introducción en la red de un simple *pendrive* puede causar graves perturbaciones en un ámbito asimétrico, debido a los grandes efectos de los ataques y el pequeño coste que requieren, sobre el que no se puede emplear la disuasión. La disuasión en la ciberguerra es más incierta que en el caso de la estrategia nuclear, ya que en este tipo de guerra no hay destrucción mutua asegurada. Mediante la introducción de virus informáticos se puede anular total o parcialmente la información que contienen las redes establecidas a nivel mundial. Estas perturbaciones pueden llegar a paralizar la vida nacional y por ello se comportan como un arma que estará presente en todos los conflictos y situaciones de crisis en el futuro, y serán una auténtica amenaza para la paz.

Unos pocos expertos, con escaso coste, pueden mantener en jaque a un Estado poderoso si encuentran una vulnerabilidad a explotar. La identificación de un atacante puede durar meses y en el caso de un grupo terrorista puede que no se tengan medios para responder. Por este motivo muchos países están desarrollando capacidades ofensivas en el ciberespacio y se estima que más de 100 centros de inteligencia llevan a cabo estas actividades. Estados Unidos ha creado un Mando para el Ciberespacio (*Ciber Command*), con un general al frente, que al parecer está integrado por 90.000 hombres.

Se trata de un nuevo concepto de guerra, cuyas acciones han aparecido desde finales del pasado siglo, que ha dado lugar a la aparición de las llamadas armas cibernéticas, genéricamente los virus, que responden a un nuevo concepto de arma. No se trata de armas de destrucción masiva, puesto que no destruyen nada a pesar de que su efecto puede llegar a ser demoledor, sino que interrumpen la actividad cibernética, por lo que se les denomina de interrupción masiva.

Conceptos fundamentales

La ciberseguridad es un componente muy importante de la Seguridad Nacional, por lo que se requiere un proceso continuo de análisis de los riesgos inherentes al ciberespacio.

El JEMAD define la Ciberdefensa Militar como «el conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control propios y la información que manejan, así como para permitir la explotación y respuesta sobre los sistemas adversarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos».

La ciberdefensa, componente muy importante de la Defensa Nacional, es multidisciplinar, ya que los ciberataques pueden afectar a ciudadanos, empresas, administración, infraestructuras críticas, sector bancario, etcétera.

Los agentes atacantes reciben diversas acepciones, tales como:

— *Virus:* programa que está diseñado para autocopiarse con la intención de infectar otros programas o ficheros. Solo infecta cuando se ejecuta o se abre el programa infectado.
— *Gusano*: es similar al virus, del que se diferencia en su forma de producir los daños. Mientras que los virus intentan infectar a otros programas, los gusanos infectan realizando autocopias con objeto de colapsar otros equipos, y se propagan automáticamente en la red con independencia de la acción humana.
— *Troyano:* Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil e inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc. Crea «puertas traseras» que permiten el acceso de usuarios no autorizados. No producen daños necesariamente. El Stuxnet es un virus de tipo troyano, creado por los Estados Unidos e Israel, que en junio de 2010 infectó equipos industriales en todo el mundo, tales como los sistemas de Control de Supervisión y de Adquisición de Datos (SCADA). Es capaz de atacar infraestructuras, por ejemplo centrales nucleares. Irán creó un antivirus contra el Stuxnet.
— *Código dañino*, también conocido como código malicioso, maligno o *malware* en su acepción inglesa. El término *malware* incluye virus, gusanos y troyanos, es anónimo, no reconoce víctimas y ataca de forma aleatoria. Es un *software* capaz de realizar un proceso no autorizado sobre un sistema, con un deliberado propósito de ser perjudicial. Infectan a otros ordenadores y se propagan automáticamente en la red con independencia de la acción humana. El término se usa genéricamente para referirse a una variedad de *software* bastante intuitiva y molesta.
— *Bomba lógica*: es parte de un programa que comprueba constantemente el cumplimiento de alguna condición lógica, por ejemplo, número de accesos o satisfacción de una cierta fecha. Cuando esto ocurre desencadena alguna acción determinada. Cuando la condición a verificar es una cierta fecha, la bomba se llama temporal. Un ejemplo se daría en una empresa en la que se introduce una clave personal por empleado, de modo que cuando cesa se le cierra el ordenador imposibilitando el acceso a toda información de la empresa. Igualmente se daría el caso contrario en el que el empleado haya conectado una bomba lógica, de modo que al cesar pueda borrar información útil a la empresa.

— *Botnet:* es un conjunto de robots informáticos que actúan automáticamente. Se emplea para enviar correos basura no solicitados con fines publicitarios (*spams*) a direcciones de correo electrónico y para descarga de ficheros que ocupan gran espacio y que consumen gran ancho de banda, o que se reciben, sin permiso o autorización del receptor y de remitentes desconocidos en la mayoría de los casos, con fines publicitarios.

Atendiendo a su autoría los ciberataques se pueden clasificar en:

— *Patrocinados por Estados*. En estos últimos años se han detectado contra las infraestructuras o contra objetivos concretos. Entre los más conocidos están el ataque a Estonia en el 2007, que supuso la inutilización temporal de muchas de sus infraestructuras críticas; los sufridos por las redes clasificadas estadounidenses, producidos por atacantes basados en China; el último ataque por virus a los sistemas informáticos de decenas de industrias iraníes, reconocido por Irán y del que dice haberse recuperado. Aquí puede también incluirse el espionaje industrial.
— *Servicios de inteligencia y contrainteligencia*. Los Estados suelen disponer de bastantes medios tecnológicos avanzados.
— *Terrorismo y extremismo político e ideológico*. Utilizan el ciberespacio para planificar sus acciones publicitarias y como herramienta de financiación.
— *Ataques de delincuencia organizada*. Su objetivo es la obtención de información para conseguir beneficios económicos.
— *Ataques de perfil bajo*. Ataques de naturaleza muy heterogénea ejecutados por personas con conocimientos TIC.

Infraestructuras críticas

Las infraestructuras críticas son el conjunto de recursos, servicios, tecnologías de la información y redes, que en caso de sufrir un ataque causarían gran impacto en la seguridad, tanto física como económica de los ciudadanos, o en el normal funcionamiento del gobierno. La criticidad de una infraestructura está fijada por los tres criterios siguientes:

— El número potencial de víctimas mortales o de lesiones graves que pueda producir.
— El impacto económico en función de las pérdidas y el deterioro de productos o servicios, incluido el posible impacto medioambiental.
— El impacto público producido por la alteración de la vida ciudadana.

Las infraestructuras críticas en España se agrupan en los 12 sectores siguientes:

— Centrales y redes de energía.
— Tecnología de la información y de las comunicaciones.
— Sistema financiero y tributario (por ejemplo banca, valores e inversiones).
— Sector sanitario.
— Espacio.
— Instalaciones de investigación.
— Alimentación.
— Agua (embalses, almacenamiento, tratamiento y redes).
— Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control de tráfico).
— Industria nuclear.
— Administración (servicios básicos, instalaciones, redes de información activas, principales lugares y monumentos nacionales).

Dependen de los sistemas de comunicaciones y por lo tanto el riesgo de interrupción por ataques cibernéticos ha aumentado considerablemente. Estas infraestructuras se detallan en un catálogo secreto, que en el caso de España se compone de 3.700 infraestructuras menores, de las que el 80 por 100 corresponden al sector privado, lo que constituye una auténtica base de datos en la que se especifican las medidas de protección, la criticidad y los planes de reacción.

En España existe el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), que depende del secretario de Estado de Seguridad (SES) del Ministerio del Interior, que es la autoridad responsable de la protección, dirección y coordinación de dichas infraestructuras. Dentro de las infraestructuras críticas de la Administración están las redes y sistemas del Ministerio de Defensa, cuya integridad es vital, ya que cualquier incidente podría poner en peligro la soberanía nacional. La integridad de las redes y sistemas de defensa, especialmente los que incluyen información clasificada, es vital para la conducción de operaciones militares, de inteligencia o las que controlan las infraestructuras críticas.

Es de gran importancia fomentar las tecnologías de la información y de las comunicaciones (TIC) mediante la coordinación entre el ámbito civil y el ámbito militar. Resulta peligroso realizar pruebas y ensayos en las redes operativas con el fin de investigar sobre la seguridad de las TIC; por ello se ha creado recientemente el Laboratorio de Ciberdefensa en el Instituto Tecnológico de la Marañosa (ITM), dependiente de la DGAM.

Características de la ciberguerra

La ciberguerra es un conflicto entre Estados tecnológicamente avanzados, que se realiza mediante ciberataques aisladamente, o como parte de una guerra convencional. No obstante los conflictos y confrontaciones en el ciberespacio pueden no ocurrir en el contexto de una guerra ni en una confrontación general. También se puede definir como el conjunto de acciones que se realizan para producir alteraciones en la información y en los sistemas del enemigo, a la vez que se protegen la información y los sistemas del atacante. Es un conflicto que usa el ciberespacio como escenario principal. Los ataques informáticos no se consideran como ataques armados.

Los ciberataques no requieren infraestructura alguna, lo que les imprime el carácter asimétrico. Existe gran dificultad para identificar y localizar al enemigo. Al no producirse destrucción alguna no existe la disuasión, como ocurre en la guerra nuclear. El espionaje es muy importante en la ciberguerra.

La frontera entre un ataque cibernético y un ataque de ciberguerra radica en la importancia de este ataque reflejado en la interrupción que produce en la vida nacional o en cualquiera de sus instituciones críticas. Un ciberataque puede dar lugar a la invocación del Artículo V por parte de la nación de la OTAN víctima cuando afecte a alguna de sus instituciones críticas.

Estrategias ofensivas y defensivas en la ciberguerra

Lo que define una estrategia son sus objetivos y sus líneas de acción y, como en toda guerra, puede ser defensiva u ofensiva. En relación con la ciberguerra, una estrategia ofensiva será la que tenga por objetivos la información y los sistemas del adversario que protegen las infraestructuras críticas, y las líneas de acción serán los distintos empleos de las ciberarmas para anularlos. Por el contrario, una ciberestrategia defensiva tendrá por objetivo la información y los sistemas propios, y las líneas de acción estarán enfocadas a la conservación de los sistemas propios, lo que redunda en la protección de las infraestructuras críticas. No obstante lo anterior, la estrategia ofensiva requiere estar preparado para defenderse de un ciberataque sofisticado.

Genéricamente las operaciones cibernéticas en redes o CNO *(Computer Network Operations)* se componen de operaciones de ataque, CNA *(Computer Network Atttack)*, Operaciones de Defensa, CND *(Computer Network Defence)*, y de operaciones de explotación, CNE *(Computer Network Explotation)*. Las CNA y CNE corresponden a una estrategia de carácter ofensivo, mientras que las CND corresponden a una estrategia de carácter defensivo.

La ciberseguridad en el ámbito militar

Desde el comienzo del siglo XXI el escenario estratégico internacional se caracteriza por la aparición de nuevas amenazas, tales como el terrorismo internacional, así como por la aparición de diferentes modalidades de ataques que se pueden producir a través del ciberespacio, poniendo de manifiesto que la superioridad militar tradicional no proporciona un factor eficaz de disuasión ni garantiza con certeza más seguridad.

Nuestra sociedad tiene una alta dependencia tecnológica que seguirá aumentando en el futuro, y las Fuerzas Armadas necesitan en tiempo real de apoyo logístico, mando y control, información de inteligencia, etc., y todas estas actividades dependen de redes informáticas. La probabilidad de sufrir ataques informáticos es muy alta, lo que puede permitir a nuestros adversarios la obtención de inteligencia valiosa sobre nuestras capacidades.

Algunas naciones, entre ellas China, Rusia, Corea del Norte e Israel, disponen de unidades especializadas con capacidad de llevar a cabo ciberataques, por lo que es necesario disponer de una capacidad de defensa ciberespacial que garantice una protección frente a estos u otros, y que al propio tiempo permita conocer y bloquear los sistemas del posible adversario. De hecho, nuestros aliados han iniciado los trabajos para adquirir dicha capacidad. No obstante, con frecuencia los ciberataques proceden de servidores residentes en países neutrales, cuyas respuestas pueden incluir consecuencias imprevistas, por lo que este tipo de reacciones debe estar siempre bajo un mando estratégico que disponga de una visión integral y global de la situación. Además, las vulnerabilidades no solo se presentan en los sistemas en red, tanto en su *software* como en su *hardware*, sino que pueden sabotearse antes de estar unidos a un sistema de explotación, ya que el código dañino y las bombas lógicas pueden insertarse en el *software* cuando se está desarrollando. En cuanto al *hardware*, se puede grabar en el *firmware* de los *chips* de los ordenadores, permitiendo su manipulación remota durante su fabricación. Este es el caso de la introducción del virus Stuxnet por parte de los Estados Unidos en el *hardware*, adquirido por Irán, de las centrifugadoras para el enriquecimiento del uranio en una central nuclear persa, lo que ha supuesto un retraso de 18 meses. El sabotaje es imposible de detectar y peor de erradicar.

La crisis económica actual, con sus restricciones en las inversiones en seguridad, tanto en las FAS como en las empresas o en las administraciones públicas, supone un grave riesgo. El Ministerio de Defensa ha publicado un documento sobre la Política de Seguridad de la Información con sus normas de aplicación, y ha emprendido una serie de iniciativas orientadas en este sentido, tanto en la red de Propósito General como en la de Mando y Control dependiente del JEMAD. La Directiva de Planeamiento Militar, promulgada por el JEMAD, estudia las capacidades con que deben contar las FAS en el ciberespacio, y el Concepto de Estrategia Militar tiene en cuenta la cibersegu-

ridad dentro del nuevo escenario estratégico y analiza las tendencias y previsiones en este campo.

La ciberdefensa en el ámbito internacional y en la OTAN

Para fortalecer la capacidad de prevención y respuesta ante incidentes informáticos se deben tomar entre otras las siguientes medidas técnicas:

— Fortalecer la infraestructura vertebral de Internet *(backbone)*.
— Ampliar las conexiones con el *World Wide Web* para que la capacidad en Internet fuese más difícil de desbordar.
— Integrar todos los servicios electrónicos del gobierno en un solo sistema centralizado.
— Ampliar la capacidad de detectar ataques cibernéticos.

En general las naciones aisladamente no tienen capacidad técnica ni jurídica para enfrentarse a ciberataques masivos, por lo tanto solo se puede abordar el problema desde la cooperación internacional.

La UE ha elaborado el Concepto de Operaciones en Red (CON), y la Agencia Europea de Defensa (EDA) gestiona su implementación. Las operaciones cibernéticas en redes son las acciones necesarias para obtener la superioridad en la información y denegarla al enemigo, que junto a las operaciones de Guerra Electrónica se emplean para interrumpir, perturbar, inutilizar, degradar o engañar los sistemas de mando y control del enemigo, anulando su capacidad para tomar decisiones eficaces y oportunas, preservando a la vez los sistemas de mando y control propios y amigos.

El 7 de enero de 2008 la OTAN publicó su Política de Ciberdefensa para proteger los sistemas de información y comunicaciones (CIS) e impulsó las siguientes acciones:

— Desarrollo del concepto de ciberdefensa.
— Protección de las redes de la OTAN.
— Integración de las ciberarmas en su Planeamiento de Defensa.
— Impulso y apoyo para establecer, en octubre de ese año, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN en Tallin (Estonia), formado por personal de 10 países, entre ellos España.
— Creación de los Equipos de Respuesta Inmediata (RRT) a los ciberataques. Estos equipos consisten en un núcleo permanente de seis expertos especializados que pueden coordinar y ejecutar misiones de respuesta. Hay también expertos nacionales o de la Alianza en áreas específicas. El número y el perfil vienen determinados por la misión a cumplir. Estos expertos se forman según los procedimientos OTAN en

el manejo de equipos y participan en un ciberejercicio que se celebra cada año.
— Creación de la Autoridad para la Gestión de la Ciberdefensa (única autoridad con responsabilidad y medios para coordinar todas las actividades de ciberdefensa y las respuestas ante los ciberincidentes), con su correspondiente estructura y organización de apoyo.
— Creación de la hoja de ruta para lograr la capacidad de respuesta.

El 20 de noviembre de 2010, la Cumbre de Lisboa creó el Nuevo Concepto Estratégico de la OTAN y la Estrategia de Ciberseguridad de la OTAN, que destacaban la necesidad de aumentar la capacidad de ciberdefensa. En marzo y junio de 2011 la OTAN aprobó respectivamente una Revisión de la Política de Ciberdefensa y un Plan de Acción de Ciberdefensa. La nueva capacidad de la OTAN en ciberdefensa es uno de los once proyectos prioritarios acordados en la Cumbre de Lisboa. También está desarrollando las normas para la protección de las Infraestructuras Críticas y el Nivel de Seguridad de los CIS. La Alianza incorporará e integrará las medidas de ciberdefensa en las misiones. El Plan de Acción de Ciberdefensa permitirá el despliegue de los nuevos niveles de ciberdefensa a principios de 2013.

La Nueva Política de Ciberdefensa de la OTAN especifica las tareas principales de los aliados, que son: llevar a cabo la defensa colectiva; gestionar las crisis; garantizar la protección de los sistemas de información y de los sistemas CIS, tanto militares como civiles, y tanto públicos como privados; implementar la coordinación en la ciberdefensa; desarrollar las capacidades y mecanismos de respuesta e incluir las medidas de ciberdefensa en las misiones, en los procesos de planeamiento de la defensa y en las estructuras de la OTAN. También se precisan los objetivos estratégicos a alcanzar, los órganos competentes y sus responsabilidades, la contribución de las instituciones de los países y el nivel tecnológico a alcanzar. Este último debe fijar los objetivos de I + D, como ya ha hecho Estados Unidos, y en menor grado el Reino Unido, que lo ha desarrollado ya a nivel militar; así como Francia, que acaba de crear su Agencia de Seguridad de los Sistemas de Información. Corea del Sur e Israel también están desarrollando y perfeccionando su ciberdefensa, mientras otros países como Rusia, China, Irán, Pakistán y Corea del Norte han reconocido su interés estratégico en el ciberespacio.

La OTAN proporcionará ayuda a los aliados que sean atacados. Cualquier nación de la OTAN que sufra un ciberataque podrá solicitar ayuda a la Alianza. El Comité de Gestión de Ciberdefensa (CDBM) considerará la petición. Si las solicitudes proviniesen de naciones no miembros tendrían que ser aprobadas por el Consejo de la Alianza.

Todos los procedimientos que se establezcan para los Equipos de Respuesta Rápida (RRT) deberán de haberse terminado en el verano de 2012 y figurarán en un manual. A finales de 2012 estará operativa la Capaci-

dad de los RRT, que tras su activación responderá dentro de las 24 horas del incidente. Se están preparando los perfiles necesarios de los expertos para misiones de asistencia según las áreas de competencia. Con los RRT, la OTAN, en cumplimiento del principio de mutua asistencia y defensa colectiva, podrá ofrecer bajo petición asistencia profesional y bien organizada a sus miembros y socios, y principalmente a aquellos países que no dispongan de recursos para establecer sus capacidades de ciberdefensa. Durante el Ciberejercicio de 2010, se practicó el mecanismo de consulta y toma de decisiones por el RRT al nivel del CDBM y se aprendieron los procedimientos de mejora.

Según fuentes de la OTAN, se ha invitado a observadores de la industria al Ciberejercicio 2012 y probablemente participarán en los próximos ciberejercicios. Para ello el grupo asesor de industria de la OTAN, EINIAG, habrá estructurado la cooperación entre la Alianza y la industria en estos temas de ciberdefensa, ya que por razones de eficacia todas las partes involucradas deben trabajar juntas: la OTAN, el sector privado y las organizaciones internacionales. La OTAN ha firmado contratos de ciberdefensa para dotarse de medios técnicos con empresas privadas. El contrato ha sido adjudicado a Nothrop Grumman por unos 58 millones de euros, e incluye el despliegue de capacidades junto con el mantenimiento. Se espera alcance la capacidad operativa completa para finales de 2012.

El centro neurálgico de la lucha de la Alianza contra el ciberdelito es el Centro de Capacidad de Respuesta ante Incidentes Informáticos de la OTAN (NCIRC) responsable de todas las instalaciones de ciberdefensa de la OTAN, que desarrollará guías de seguridad y aconsejará sobre la protección de los ordenadores y las redes de información de la OTAN para reducir sus vulnerabilidades.

Cronología de los ataques cibernéticos más significativos

Por su importancia se exponen con mayor extensión los principales ataques en los últimos tiempos, que por sus consecuencias podrían considerarse como ciberguerras:

— *1999. Guerra de Kosovo*. Solo como una demostración de fuerza, más de 450 expertos informáticos de diferentes naciones consiguieron penetrar en los ordenadores estratégicos de la OTAN, de la Casa Blanca y del portaaviones *Nimitz* de la US Navy. Sirvió como grupo coordinador de actividades contra la guerra fuera de Yugoslavia, actuando como fuente alternativa de información en Internet.
— *2003. Irak*. Antes del primer ataque los norteamericanos lanzaron un ciberataque (con un gusano troyano) que impidió la salida de la aviación iraquí.

— *2003. Taiwán*. Sufrió un ataque, progresivo y aparentemente organizado que, además de un ataque de denegación de servicios (DDoS), incluyó virus troyanos y dejó sin servicios a infraestructuras, tales como hospitales, la Bolsa y algunos sistemas de control de tráfico, lo que provocó un caos. Se culpó a China.

— *2007. El cibercaso de Estonia*. En Estonia existía un clamor antirruso que estalló como un auténtico conflicto civil, fomentado por Rusia, que había visto con desagrado la incorporación de Estonia a la OTAN en 2004. La embajada de Estonia en Moscú estuvo bloqueada durante una semana sin que la policía rusa interviniese, y sufrió un ataque durante una rueda de prensa. Los enfrentamientos no fueron espontáneos, sino que contaron con la complicidad de las autoridades rusas.

  Los ciberataques tuvieron lugar entre el 27 de abril y 18 de mayo del 2007. Durante este periodo variaron su objetivo, su volumen y método, pero en líneas generales se pueden considerar dos fases: la primera fase tuvo lugar entre el 27 y 29 de abril; en ella se emplearon herramientas de ciberataque rudimentarias por parte de *hacktivistas* sin grandes conocimientos técnicos emplazados en sitios *web,* mayoritariamente rusos, contra sitios *web* de Estonia, especialmente del Gobierno, del Ministerio de Defensa y de los principales partidos políticos. La alarma surgió cuando reunido el Gobierno apercibió que no podía cargar los comunicados de prensa en sus sitios *web* oficiales.

  Una vez confirmado que el país se encontraba bajo un ciberataque, el Gobierno procedió de una manera inmediata a organizar un equipo de respuesta, liderado y coordinado por el Equipo Nacional de Respuesta ante Incidentes Informáticos (Estonian-CERT), compuesto por personal experto de los Ministerios de Comercio y Comunicaciones y de Defensa, así como de los Servicios de Inteligencia. Este fue el gran triunfo de Estonia al identificar la gravedad del asunto con celeridad y organizar inmediatamente un equipo de respuesta multidisciplinar e investirle de la autoridad necesaria.

  En la segunda fase, del 30 de abril hasta el 18 de mayo, los ataques se volvieron más complejos, más sofisticados, con uso de grandes *botnets* con una coordinación minuciosa y precisa. Con listas de objetivos y calendarios en los que indicaban hora y lugar del ataque para conseguir un enorme volumen de repeticiones simultáneas sobre los mismos servicios informáticos con el objeto de dejarlos fuera de servicio.

  Un aspecto interesante fue la relación entre la situación política y los ciberataques. Como ejemplo revelador se puede citar la coincidencia de la fiesta nacional rusa con el espectacular incremento de los ataques, ya que se registraron 128 ataques de denegación de servicio (DDoS), consistentes en hacer inaccesible un determinado servicio a los usuarios. En general se necesita un número muy grande de atacan-

tes ejerciendo peticiones de servicio sobre un mismo objetivo para conseguir la pérdida de conectividad de la red de la víctima por el consumo de su ancho de banda o sobrecarga de los recursos de los ordenadores.

Otro tipo de ataque consistía en acceder a un sitio *web* con el objetivo de modificar el aspecto visual. Atacaron sitios *web* oficiales, cambiando sus contenidos originales por otros de carácter apologético de la causa rusa y en lengua rusa. Los ataques estuvieron bien organizados, basados en el envío masivo de correos electrónicos, generados por robots, a direcciones oficiales gubernamentales y direcciones privadas de personalidades relevantes. Este ataque es más sencillo si se realiza contra un país como Estonia, país pequeño en el que un ataque masivo puede provocar una crisis de seguridad nacional, ya que la actividad política se realiza principalmente a través de las tecnologías de la información, se sigue una política de transparencia cibernética que obliga a publicar todas las direcciones de correo electrónico y *webs* de todos los servicios públicos y se emplea mayoritariamente Internet para las transacciones económicas. Al propio tiempo sirvió para la comprobación de la fortaleza y la capacidad cibernética de la OTAN.

Los spams sobrecargaban los servidores y ocupaban todo el ancho de banda, por lo que se vio obligada a solicitar un aumento del ancho de banda con 110 *megabytes* por segundo, el máximo disponible, que no era suficiente para mantener los servicios operativos. En el estudio descubrieron que la mayoría de las peticiones procedía de Egipto, seguido por Vietnam y Perú, por lo que se cortó la conexión con el extranjero. Se recuperó el ancho de banda inmediatamente y el servicio comenzó a funcionar pero solo en Estonia, y la prensa no podía informar al mundo de lo que estaba pasando. Para hacer frente a este ataque masivo no hubo más remedio que cortar la conexión con el extranjero de bancos y organizaciones gubernamentales.

El ministro de Defensa estonio informó inmediatamente de la situación a sus aliados de la OTAN y de la Unión Europea, que cooperaron para anular los *botnets*. Estonia amplió gradualmente su ancho de banda, sin revelar su capacidad ante la monitorización de su red por los atacantes. De este modo impedían modificar sus ataques de acuerdo con la inteligencia obtenida. Con objeto de proporcionar apoyo técnico visitaron Estonia observadores de los CERT de los centros de nacionales de los Estados Unidos y de la OTAN. El CERT nacional de Finlandia fue especialmente útil para llevar a cabo la cooperación internacional entre los CERT nacionales.

Después del ataque, Estonia tomó una serie de medidas para fortalecer la capacidad de prevención y respuesta ante incidentes informáticos;

entre ellas cabe destacar el desarrollo de su Estrategia Nacional de Ciberdefensa.

Estonia extrajo las tres lecciones siguientes de respuesta política ante un ciberataque masivo:

- El Gobierno identificó desde el primer momento el ataque de gran dimensión que podría llegar a ser una crisis de seguridad nacional.
- Organizó un equipo multifuncional coordinador de la respuesta con técnicos expertos, políticos, militares, diplomáticos y jurídicos.
- Reconoció ante el mundo que estaban bajo ataques cibernéticos.

El ciberataque a Estonia en el 2007 representó un hito y un reto histórico para la OTAN y puede considerarse como la primera acción de ciberguerra. Representa la primera ocasión en que un Estado miembro solicita apoyo a la OTAN por un ataque a la infraestructura crítica de información del país. Quedó demostrado que la OTAN carecía de un plan de acción para el caso de un ciberataque a un estado miembro, ya que hasta entonces se había considerado que se trataba de un problema de índole nacional, puesto que diariamente muchas naciones de la OTAN, entre ellas los Estados Unidos, reciben ciberataques semejantes o de mayor importancia. Sin embargo el caso del ataque a Estonia, debido a la dimensión del país, fue más grave, ya que puso en peligro su seguridad.

La OTAN después de los ataques a Estonia realizó un estudio y análisis, y elaboró un informe de lecciones aprendidas. Concluyó con que no solo no disponía de un plan de acción en caso de ciberataque, sino que ni siquiera disponía del concepto de ciberdefensa ni de una línea de actuación.

— *2008. Lituania*. La Agencia Tributaria Estatal quedó bloqueada por peticiones masivas, quedando durante varias horas interrumpido el servicio. Al parece el cibertataque procedía de Rumanía.

— *El cibercaso de Georgia*. Osetia del Sur, territorio del Cáucaso en la frontera entre la Federación Rusa y Georgia, que durante la época soviética tenía la consideración de *oblast* autónomo, declaró unilateralmente en 1989 su independencia tras vencer en una guerra a Georgia, convirtiéndose de facto en una republica independiente; pero tanto Georgia como la mayor parte de la Comunidad Internacional no la reconocieron.

El 7 de agosto de 2008 estalló la guerra entre Georgia por un lado y Osetia del Sur, Abjasia y Rusia por el otro, con un ataque por sorpresa por parte de Georgia. Este hecho provocó la reacción de Rusia, que lo consideró un ultraje contra ciudadanos rusos fuera de sus fronteras, por lo que al día siguiente iniciaron operaciones militares en territorio

de Osetia del Sur. El 12 de agosto finalizó la guerra mediante el plan de paz propuesto por la Unión Europea, por lo que las fuerzas volvieron a las posiciones iniciales anteriores al conflicto.
Los ciberataques contra Georgia se produjeron en tres fases:

- Fase de ataque a pequeña escala entre junio y el 7 de agosto de 2008, consistente en ataques DDoS, dos meses antes de la iniciación del conflicto.
- Conflicto armado, del 7 al 12 de agosto del 2008. Ataques bien organizados y coordinados. Durante los cinco días se sucedieron ataques contra los sitios *webs* pertenecientes al presidente de la República de Georgia, al Parlamento, al Ministerio de Defensa y Asuntos Exteriores, al Banco Nacional y a las principales agencias de noticias. El primer ataque a gran escala, con un alto grado de sofisticación, se produjo simultáneamente con la primera ofensiva de las fuerzas rusas en Georgia. Los ataques debilitaron la capacidad de toma de decisiones político-militares y la capacidad de información y de comunicaciones entre el gobierno y los ciudadanos, a la vez que a través de la ciberpropaganda trataban de influenciar en la opinión pública hacia la postura de los adversarios.
- Posconflicto, del 13 al 28 de agosto del 2008. Ataques a menor escala. Disminuyeron en número y en intensidad y su cese se debió a su falta de rentabilidad. Por un lado, las medidas de ciberdefensa lograron bloquear gran parte de ellos y por otro el entusiasmo de los ciberactivistas disminuyó después de la finalización del conflicto armado.

Los tipos de ataques, que fueron parecidos a los de Estonia de 2007, no sofisticados pero sí muy efectivos, y que influyeron en el desarrollo de las operaciones militares, consistieron en:

- Ataques prolongados y múltiples contra sitios *webs* oficiales.
- Ataques DDoS a través de *botnets* con centros de mando y control dispersos en diferentes países, no especialmente sofisticados, técnica y operativamente mejor organizados y coordinados, con mayor poder dañino y con un mayor número de participantes que en el caso de Estonia.
- Ataques no especialmente sofisticados pero bien planeados y organizados que se basaban en reconocimientos de objetivos y evolución continua de los ataques de acuerdo con la inteligencia obtenida. Las redes sociales fueron ampliamente utilizadas para reclutar voluntarios y para la descarga de *malwares*.

Los objetivos consistían en causar pérdida operativa y de confianza en las instituciones políticas, militares y financieras y bloquear la capacidad de comunicación entre las instituciones, el gobierno y los ciudadanos, y entre Georgia y el mundo exterior.

Georgia disponía de poca capacidad técnica para enfrentarse a los ciberataques, por lo que la cooperación internacional pública y privada fue fundamental. La respuesta técnica básicamente fue el traslado de los sitios *webs* a otras plataformas fuera de las fronteras. Georgia tuvo gran facilidad para conseguir apoyo multinacional debido a, los precedentes de Estonia y de Lituania. Estonia envió expertos del CERT-EE con el fin de ayudar a la respuesta técnica y con resultado positivo, y ofreció infraestructura para alojar sitios *webs* oficiales de Georgia.

Como en Estonia, la participación del gobierno ruso no ha sido probada hasta la fecha, aunque al parecer sí su complicidad en la participación de los ataques. Esto se fundamenta en tres hechos: la falta de cooperación de Rusia en la identificación de los responsables; Rusia es el principal o único beneficiario de los resultados de la ofensiva cibernética; y los ciberataques evolucionaban acorde con la evolución de las operaciones armadas, y para ello se necesitaba información solo disponible por las autoridades políticas y militares rusas.

— *2009. Kirguistán*. Sufrió el primer ciberataque.
— *2010. Irán*. Registró un ataque a las centrifugadoras del programa de enriquecimiento de uranio, acusando a los Estados Unidos de su autoría. Aparentemente Estados Unidos introdujo virus en el *hardware* de equipos suministrados para las citadas centrifugadoras. El virus empleado fue el Stuxnet, cuyo origen era Israel y los Estados Unidos.
— *2011. Canadá*. Los sistemas de contraseña del Ministerio de Finanzas sufrieron un ciberataque procedente de China.
— *2012. Medio Oriente*. En mayo de 2012 se ha descubierto uno de los *malware* más dañinos hasta la fecha llamado Flame o Skywiper, el cual se especula que está diseñado para propósitos de ciberespionaje, Entre los países más afectados están Irán, Israel, Sudán, Libia, Arabia Saudí y Egipto.

  El virus Flame podría estar cinco años circulando, está diseñado para recopilar y robar información estratégica y se tata del *software* de espionaje más complejo que se ha descubierto, diseñado para espiar a los usuarios de los ordenadores que infecta. Puede robar documentos, realizar capturas de pantallas de los programas que infecta y grabar conversaciones de servicios de mensajerías. Es una mezcla de troyano y gusano, se le pueden añadir módulos y modificar sobre la marcha. Es una herramienta maliciosa con una configuración muy compleja, diferente al Stuxnet, puesto que no destruye sino que espía de una manera invisible, por lo que es más peligroso y difícil de detectar, e

infecta áreas vulnerables semejantes a las del Stuxnet, propagándose de igual forma. Según la agencia rusa Karpersky, su desarrollo costó unos 100 millones de dólares. Es el cibervirus más complejo de la actualidad, 20 veces más potente que el Stuxnet, y es obra de un Estado y no de cibercriminales comunes.

El origen de la mayor parte de los ciberataques que sufre el Reino Unido, según el propio Gobierno, proceden de Rusia y China. Los servicios secretos rusos llevan años perfeccionando la forma de atacar páginas *webs*, penetrar o paralizar los sistemas informáticos, perturbar las telecomunicaciones, bloquear los servicios públicos e interceptar correos electrónicos.

Otras acciones recientes

La OTAN declaró oficialmente su compromiso con el fortalecimiento de los Sistemas de Información Crítica contra los ciberataques y de establecer capacidades de apoyo a las naciones previa petición.

Estados Unidos ha secuestrado portales *webs* islamistas, donde han sustituido textos de apoyo a la *yihad* por detalladas descripciones de cómo Al Qaeda aniquila a civiles. Para ello ha formado un grupo de avezados *hackers*, constituido por un equipo de expertos informáticos en la red, que hablan urdu, árabe o somalí, vigilan en Internet, y emplean las redes sociales y otros instrumentos para anular la propaganda de Al Qaeda mediante la exhibición de los ataques brutales de esta contra civiles. La CIA y el Centro de Comunicaciones Estratégicas, que emplea a unas 40 personas y está operativo desde el 10 de septiembre del 2011 con un presupuesto de 4,7 millones de euros, se han infiltrado en las redes islamistas. El Mando Cibernético creado en mayo del 2010 gestionará los recursos destinados a salvaguardar las redes de seguridad norteamericanas. La secretaria de Estado norteamericana ha declarado que emplean las redes sociales para dejar al desnudo las contradicciones cibernéticas en la propaganda de Al Qaeda. El Centro de Comunicaciones Estratégicas, en el que participan expertos informáticos del Pentágono y sus Comandos de Operaciones Especiales, se ha infiltrado en una red islamista de Yemen que trataba de la aniquilación de norteamericanos e que introdujo en ella diversas muestras de los ataques terroristas de Al Qaeda; en el sitio *web* original había fotos de ataúdes cubiertos con banderas norteamericanas y que los *hackers* del Departamento de Estado sustituyeron por otros cubiertos con banderas yemeníes. El grupo terrorista de Al Qaeda emplea Internet para difundir los vídeos de sus ciberterroristas. La revista de su aliado en la península Arábiga, INSPIRE, comparte información en la red sobre el enemigo y sobre el modo de atacar eficazmente a los Estados Unidos. Actualmente y desde hace cinco

años, como un claro ejemplo de ciberespionaje, existen unos 600 ordenadores infectados en Israel, Palestina, Siria, Sudán y Egipto.

Conclusiones

- El ciberespacio es el único de los *Global Commons* creado artificialmente por el hombre y carece de fronteras geográficas.
- En el ciberespacio la amenaza procede fundamentalmente de los Estados, del ciberterrorismo y del crimen organizado, ante lo que no funciona la disuasión.
- La ciberseguridad está incluida en la Seguridad Nacional y la ciberdefensa en la Defensa Nacional.
- La ciberdefensa afecta tanto a la Defensa Civil como a la Defensa Militar y afecta cada vez más a un ámbito multidisciplinar.
- En el Nuevo Concepto Estratégico de la OTAN destaca la necesidad de incrementar la capacidad de ciberdefensa.
- La OTAN carece de capacidad orgánica para parar y disuadir ciberataques.
- A nivel internacional, la ciberdefensa debe incluirse también en las estrategias de defensa colectiva.
- El resultado de la Política de Ciberdefensa de la OTAN es la creación de los Equipos de Respuesta (RRT).
- Los ataques cibernéticos cada vez serán más frecuentes y más complejos.
- La ciberguerra es asimétrica.
- La obtención de las capacidades cibernéticas debe integrarse en la Doctrina Militar.
- La superioridad militar tradicional no proporciona un factor eficaz de disuasión ni garantiza eficazmente más seguridad.
- La OTAN, desde la Cumbre de Lisboa de 2010, ha intensificado su actividad en relación con la ciberguerra, e incluye las medidas a adoptar por la Ciberdefensa en el planeamiento de Defensa.
- Es necesario crear un centro de experimentación en ciberseguridad y ciberdefensa.

BIBLIOGRAFÍA

Publicación número 149 del Instituto Español de Estudios Estratégicos, titulada *Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*.
Distintas informaciones publicadas en Internet, prensa y revistas.
Publicaciones no clasificadas del Ministerio de Defensa.
Información verbal directa de expertos de la Armada.